

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-92046

(P2000-92046A)

(43) 公開日 平成12年3月31日 (2000.3.31)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード (参考)
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 D 5 B 0 4 3
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 F 5 B 0 8 5
G 0 6 T 7/00		15/62	4 6 0 5 J 1 0 4
H 0 4 L 9/14		H 0 4 L 9/00	6 4 1
			6 7 3 A

審査請求 未請求 請求項の数 7 O L (全 16 頁) 最終頁に続く

(21) 出願番号 特願平10-257813

(22) 出願日 平成10年9月11日 (1998.9.11)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 中村 浩

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 馬場 義昌

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74) 代理人 100102439

弁理士 宮田 金雄 (外2名)

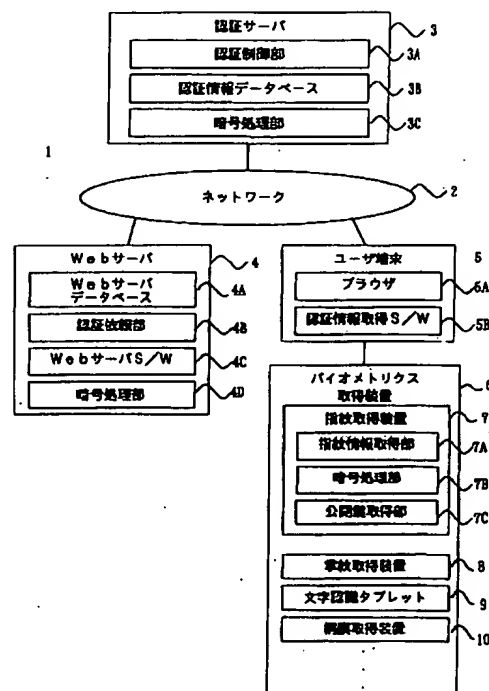
最終頁に続く

(54) 【発明の名称】 遠隔認証システム

(57) 【要約】

【課題】 バイオメトリクス情報により個人の認証を行う際、ユーザの個人情報であるバイオメトリクス情報を保護した上で確実に認証が受けられるとともに、セキュリティ上強固な遠隔認証システムおよび遠隔認証方法を得る。

【解決手段】 ユーザの個人情報であるバイオメトリクス情報を暗号化し、バイオメトリクス情報はユーザの指定した認証サーバにのみ復号可能な状態でネットワーク上を転送するので、バイオメトリクス情報というユーザ個人のプライバシーを、ユーザの意志を反映した形で確実に保護できると共に、認証サーバで認証情報作成時の日時が確認できるため、不正な認証情報の再使用が防止でき、さらに認証サーバによって認証されたかが認証依頼側で確認できるためシステムのセキュリティを高く保つことが可能である。



【特許請求の範囲】

【請求項 1】 ネットワークに、認証サーバと、アプリケーションサーバと、ユーザ端末がそれぞれ接続され、前記ユーザ端末を使用するユーザの認証を行う遠隔認証システムにおいて、

前記認証サーバは公開鍵暗号方式の公開鍵と秘密鍵の組を所持し、公開鍵を公開し、秘密鍵を秘匿しており、前記ユーザ端末には少なくとも 1 つ又は複数種類のバイオメトリクス取得装置が接続され、

前記バイオメトリクス取得装置は、認証に際して取得したユーザのバイオメトリクス情報を、共通鍵暗号方式の共通鍵で暗号化し、

日時情報を取得し、日時情報と前記共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに前記共通鍵で暗号化し、

ユーザの指定する認証サーバの公開鍵を取得し、前記共通鍵を前記認証サーバの公開鍵で暗号化すると共に、暗号化した前記バイオメトリクス情報と暗号化した前記共通鍵と日時情報と、日時情報と前記共通鍵を連結してメッセージダイジェストを暗号化したものを認証情報として前記ユーザ端末へ転送し、

前記ユーザ端末と前記アプリケーションサーバは、該認証情報を前記認証サーバへ転送し、前記認証サーバは、転送された認証情報を前記秘密鍵で復号を行って得た前記共通鍵により、ユーザのバイオメトリクス情報を復号し、該バイオメトリクス情報によってユーザを認証し、認証した結果と認証した結果のメッセージダイジェストを前記秘密鍵で暗号化し、共に前記アプリケーションサーバに転送することを特徴とする遠隔認証システム。

【請求項 2】 ネットワークに認証サーバと、ユーザ端末がそれぞれ接続され、前記ユーザ端末を使用するユーザの認証を行う遠隔認証システムにおいて、前記認証サーバは公開鍵暗号方式の公開鍵と秘密鍵の組を所持し、公開鍵を公開し、秘密鍵を秘匿しており、前記ユーザ端末には少なくとも 1 つ又は複数種類のバイオメトリクス取得装置が接続され、

前記バイオメトリクス取得装置は、認証に際して取得したユーザのバイオメトリクス情報を、共通鍵暗号方式の共通鍵で暗号化し、日時情報を取得し、日時情報と共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに共通鍵で暗号化し、ユーザの指定する前記認証サーバの公開鍵を取得し、前記共通鍵を前記認証サーバの公開鍵で暗号化すると共に、前記暗号化したバイオメトリクス情報と暗号化した共通鍵と日時情報と、日時情報と共通鍵を連結してメッセージダイジェストを暗号化したものを認証情報として前記ユーザ端末へ転送し、

前記ユーザ端末は該認証情報を前記認証サーバへ転送し、

前記認証サーバは、転送された認証情報を前記秘密鍵で

復号を行って得た前記共通鍵により、ユーザのバイオメトリクス情報を復号し、該バイオメトリクス情報によってユーザを認証し、認証した結果と認証した結果のメッセージダイジェストを前記秘密鍵で暗号化し、共に前記ユーザ端末に転送することを特徴とする遠隔認証システム。

【請求項 3】 前記バイオメトリクス取得装置は、認証に際して、暗号化せずにバイオメトリクス情報を前記ユーザ端末へ転送し、

10 前記ユーザ端末は、取得したユーザのバイオメトリクス情報を、共通鍵暗号方式の共通鍵で暗号化し、ユーザの指定する認証サーバの公開鍵を取得し、前記共通鍵を前記認証サーバの公開鍵で暗号化し、日時情報を取得し、日時情報と共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに前記共通鍵で暗号化すると共に、前記暗号化したバイオメトリクス情報と前記暗号化した共通鍵と日時情報と、日時情報と共通鍵を連結してメッセージダイジェストを暗号化したものを認証情報として前記ユーザ端末へ転送することを特徴とする請求項 1 または請求項 2 に記載の遠隔認証システム。

【請求項 4】 前記ユーザ端末は、認証に際して、取得したユーザのバイオメトリクス情報を暗号化する共通鍵暗号方式の共通鍵を生成する場合、前記共通鍵生成のための乱数の一部または全部に該バイオメトリクス情報を使用することを特徴とする請求項 1 ～ 3 のいずれかに記載の遠隔認証システム。

【請求項 5】 前記バイオメトリクス取得装置は、バイオメトリクス取得装置を管理する管理者の認証部と、バイオメトリクス取得装置を初期化する初期化者の認証部を含み、

前記 2 つの認証部は独立して認証し、前記管理者が認証されない場合でも、前記初期化者の認証で初期化することを特徴とする請求項 1 ～ 3 のいずれかに記載の遠隔認証システム。

【請求項 6】 前記認証サーバは、ユーザ認証時に、バイオメトリクスを照合した結果の照合率の履歴を記憶し、ユーザ認証に際して、本人と同一でない場合には、前回までのユーザを本人と同一とした時の平均照合率と比較し、今回の照合率が前記管理者の定める規定値以上に大きく変動しているかを確認し、該既定値以上の大きな変動での失敗回数が前記管理者の定める既定値以上に達した場合には、予め登録されている連絡先に通知することを特徴とする請求項 1 ～ 3 のいずれかに記載の遠隔認証システム。

【請求項 7】 前記認証サーバは、ユーザ認証時に、バイオメトリクスを照合した結果の照合率の履歴を記憶し、ユーザ認証に際して、本人と同一した場合には、前回までのユーザを本人と同一とした時の照合率と比較し、同一の照合率であり、バイオメトリクス情報のメッセー

3

ジダイジェストが格納されていない場合にはユーザ認証を失敗させ、今回のバイオメトリクス情報のメッセージダイジェスト算出し、照合率とともに記憶し、同一の照合率で、メッセージダイジェストが格納されている場合には、今回のバイオメトリクス情報のメッセージダイジェストを算出して照合率と組で記憶するとともに、過去の同一の照合率におけるバイオメトリクス情報のメッセージダイジェストと比較し、異なれば本人と同一とし、今回の照合率とメッセージダイジェストの組が過去の照合率とメッセージダイジェストの組と完全に一致した場合には本人と同一しないと、過去の照合率とメッセージダイジェストの組と完全に一致する場合が、管理者が定める既定値以上に達した場合には、予め登録されている連絡先に通知することを特徴とする請求項 1～3 のいずれかに記載の遠隔認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、バイオメトリクスにより個人の特定を行う遠隔認証システムに関するものである。

【0002】

【従来の技術】従来、ネットワークに接続された情報処理システムにおいて機密保持のため、個人を特定し該個人のアクセス許可と不許可の判断を行なう、すなわち認証が必要である。また、銀行の現金自動支払機等では個人の特定と預金残高など該個人の取り引き情報にアクセスするための認証や、機密度の高い研究場所や会員制クラブなどへの入室時にも個人の認証が実施されている。

【0003】これらの認証として、身分証明書などと同様の位置づけである、磁気カードや IC カードやパスワードなどの個人の記憶やこれらの組み合わせによって個人の特定と資格の認定、すなわち認証を実施している。パスワードなどは忘却の恐れや、磁気カード、IC カードなどは紛失、破壊などにより認証が不能に陥ったり、盗難やパスワード情報の漏洩により本人以外が本人と成りすまして認証されてしまうなどの問題がある。

【0004】また、ネットワーク上でユーザを認証する手段の 1 つに、ユーザの作成したメッセージを認証し、間接的にユーザを認証するデジタル署名がある。デジタル署名では、まずメッセージの送り手がメッセージの原文を圧縮したメッセージダイジェストを送り手の暗号鍵で暗号化した暗号文をメッセージに添付する。メッセージの受け手は、受け取ったメッセージからメッセージダイジェストを作成し、また送り手の復号鍵で添付された暗号文からメッセージダイジェストを復号してこれら 2 つのメッセージダイジェストが一致することで、送り手本人が送ったメッセージであることと、改竄されていないことを確認する。

【0005】また、前記暗号方式には、暗号鍵と復号鍵

4

に同一の鍵を用いる共通鍵暗号方式と暗号鍵と復号鍵とが異なる公開鍵暗号方式が存在する。公開鍵暗号方式では、一方の鍵を秘密鍵とし安全に保管し、もう一方の鍵を公開鍵として公表する場合、公開鍵で暗号化された暗号文は秘密鍵を所持していなければもとのメッセージへ復号できないため、送り手は希望する受け手にのみ復号できる形でメッセージを転送でき、秘密鍵で暗号化された暗号文は公開鍵でもとのメッセージへ復号ができるため、秘密鍵を所持している送り手本人からのメッセージであることを受け手が認証できる。

【0006】

【発明が解決しようとする課題】従来、IETF (Internet Engineering Task Force) の RFC (Request For Comment) に登録されている RFC1421, RFC1422 (PEM: Privacy Enhancement for Internet Electronic Mail) では、前記デジタル署名とメッセージの暗号化を公開鍵暗号方式と共通鍵暗号方式によって行っているが、送り手は自分の秘密鍵を使用するため、送り手の責任で秘密鍵を管理する必要あり、例えばフロッピーディスクや磁気カード、IC カードなどに格納して安全に所持しなければならないという問題があった。

【0007】一方、指紋情報、掌紋情報、筆跡情報、網膜情報など個人の生体的特徴であるバイオメトリクス情報による認証では、成りすましが困難であることと、ユーザ本人がいれば前記秘密鍵の情報などを管理する必要がなく、また前記磁気カードや IC カードなどで個人を認証する場合の携行品所持の煩雑さや紛失による脅威や、前記パスワード認証時の記憶の煩雑さを解消できるが、バイオメトリクス情報による認証が広域で必要な場合には、集中的なバイオメトリクス情報の管理と認証する機器が必要であり、プライバシー保護の面からユーザのバイオメトリクス情報を認証を行う機器に転送する際には秘匿などを行いセキュリティを確保しなければならないという問題があった。

【0008】また、バイオメトリクス情報を秘匿するために使用する暗号鍵を生成するようなシステムでは、一般に暗号鍵の生成に乱数を使用するが、該暗号鍵の解読を困難にするためには該乱数の傾向をなくすることが重要であるという問題もある。

【0009】また、バイオメトリクスを取得する装置は、ユーザのプライバシーの保護の面から適切に管理しなければならない、管理者の認証を行う必要があるが、この管理者の認証にバイオメトリクスを用いた場合には管理者の代行が他人はできないため、他の人は初期化も含め、バイオメトリクス取得装置に全くアクセスできなくなるという問題があった。また、正当な管理者であっても認証に使用しているバイオメトリクスが事故により傷害を受け、大きく変わってしまった、なくなってしまう

う場合などには正当な管理者であっても、初期化を含め、バイオメトリクス取得装置に全くアクセスできなくなるという問題があった。

【0010】また、一般にユーザ認証を行うシステムでは、不正な認証を早期発見が求められ、例えば銀行のキャッシュカードなどでは規定回数パスワードによる認証が失敗すると該キャッシュカードを使用不能にするなどの手段を持っている。バイオメトリクスによりユーザを認証するシステムでも、不正な認証を早期発見する必要があるが、個人毎にバイオメトリクスの状態が異なり、例えば指紋照合により個人を認証するシステムでは、本人と同定する最低の照合率が決まっているが、指が荒れていたり摩り減っている人などはその時点で最良のバイオメトリクス情報が取得できても照合率低く、指の密着不足などちょっとした取得時の失敗によりさらに照合率が低下すると、認証自体が失敗する確立が高くなり、全ての人に対して規定回数だけで不正認証と判断することが公平にできないという問題があった。

【0011】この発明は前記のような問題点を解決するためになされたもので、バイオメトリクス情報により個人の認証を行う際、ユーザの個人情報であるバイオメトリクス情報を保護した上で確実に認証が受けられるとともに、セキュリティ上強固な遠隔認証システムおよび遠隔認証方法を得ることを目的とする。

【0012】

【課題を解決するための手段】第1の発明に係る遠隔認証システムは、ネットワークに認証サーバと、アプリケーションサーバと、ユーザ端末がそれぞれ接続され、前記ユーザ端末を使用するユーザの認証を行う遠隔認証システムにおいて、認証サーバは公開鍵暗号方式の公開鍵と秘密鍵の組を所持し、公開鍵を公開し、秘密鍵を秘匿しており、前記ユーザ端末には少なくとも1つ又は複数種類のバイオメトリクス取得装置が接続され、バイオメトリクス取得装置は、認証に際して取得したユーザのバイオメトリクス情報を、共通鍵暗号方式の共通鍵で暗号化し、日時情報を取得し、日時情報と共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに共通鍵で暗号化し、ユーザの指定する認証サーバの公開鍵を取得し、前記共通鍵を前記認証サーバの公開鍵で暗号化すると共に、暗号化したバイオメトリクス情報と暗号化した共通鍵と日時情報と、日時情報と共通鍵を連結してメッセージダイジェストを暗号化したものを認証情報としてユーザ端末へ転送し、ユーザ端末とアプリケーションサーバは、該認証情報を認証サーバへ転送し、認証サーバは、転送された認証情報を前記秘密鍵で復号を行って得た前記共通鍵により、ユーザのバイオメトリクス情報を復号し、該バイオメトリクス情報によってユーザを認証し、認証した結果と認証した結果のメッセージダイジェストを秘密鍵で暗号化し、共にアプリケーションサーバに転送するものである。

【0013】また、第2の発明に係る遠隔認証システムは、ネットワークに認証サーバと、ユーザ端末がそれぞれ接続され、前記ユーザ端末を使用するユーザの認証を行う遠隔認証システムにおいて、認証サーバは、公開鍵暗号方式の公開鍵と秘密鍵の組を所持し、公開鍵を公開し、秘密鍵を秘匿しており、前記ユーザ端末には少なくとも1つ又は複数種類のバイオメトリクス取得装置が接続され、バイオメトリクス取得装置は、認証に際して取得したユーザのバイオメトリクス情報を、共通鍵暗号方式の共通鍵で暗号化し、日時情報を取得し、日時情報と共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに共通鍵で暗号化し、ユーザの指定する認証サーバの公開鍵を取得し、前記共通鍵を前記認証サーバの公開鍵で暗号化すると共に、暗号化したバイオメトリクス情報と暗号化した共通鍵と日時情報と、日時情報と共通鍵を連結してメッセージダイジェストを暗号化したものを認証情報としてユーザ端末へ転送し、ユーザ端末は該認証情報を認証サーバへ転送し、認証サーバは、転送された認証情報を前記秘密鍵で復号を行って得た前記共通鍵により、ユーザのバイオメトリクス情報を復号し、該バイオメトリクス情報によってユーザを認証し、認証した結果と認証した結果のメッセージダイジェストを秘密鍵で暗号化し、共にユーザ端末に転送するものである。

【0014】また、第3の発明に係る遠隔認証システムは、バイオメトリクス取得装置が、認証に際しては、暗号化せずにバイオメトリクス情報をユーザ端末へ転送し、ユーザ端末が取得したユーザのバイオメトリクス情報を、共通鍵暗号方式の共通鍵で暗号化し、日時情報を取得し、日時情報と共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに共通鍵で暗号化し、ユーザの指定する認証サーバの公開鍵を取得し、前記共通鍵を前記認証サーバの公開鍵で暗号化すると共に、暗号化したバイオメトリクス情報と暗号化した共通鍵と日時情報と、日時情報と共通鍵を連結してメッセージダイジェストを暗号化したものを認証情報として転送するものである。

【0015】また、第4の発明に係る遠隔認証システムは、認証に際して、取得したユーザのバイオメトリクス情報を暗号化する共通鍵暗号方式の共通鍵を生成するための乱数の一部または全部に該バイオメトリクス情報を使用するものである。

【0016】第5の発明に係る遠隔認証システムは、バイオメトリクス取得装置が、バイオメトリクス取得装置を管理する管理者の認証部と、バイオメトリクス取得装置を初期化する初期化者の認証部を含み、前記2つの認証部は独立して認証し、管理者が認証されない場合でも、初期化者の認証で初期化だけは実施できるものである。

【0017】第6の発明に係る遠隔認証システムは、

認証サーバが、ユーザ認証時に、バイオメトリクスを照合した結果の照合率の履歴を記憶し、ユーザ認証に際して、本人と同定しない場合には、前回までのユーザを本人と同定した時の平均照合率と比較し、今回の照合率が管理者の定める規定値以上に大きく変動しているかを確認し、該既定値以上の大きな変動での失敗回数が管理者の定める既定値以上に達した場合には、予め登録されている連絡先に通知するものである。

【0018】また、第7の発明に係わる遠隔認証システムは、認証サーバが、ユーザ認証時に、バイオメトリクスを照合した結果の照合率の履歴を記憶し、ユーザ認証に際して、本人と同定した場合には、前回までのユーザを本人と同定した時の照合率と比較し、同一の照合率であり、バイオメトリクス情報のメッセージダイジェストが格納されていない場合にはユーザ認証を失敗させ、今回のバイオメトリクス情報のメッセージダイジェスト算出し、照合率とともに記憶し、同一の照合率で、メッセージダイジェストが格納されている場合には、今回のバイオメトリクス情報のメッセージダイジェストを算出して照合率と組で記憶するとともに、過去の同一の照合率におけるバイオメトリクス情報のメッセージダイジェストと比較し、異なれば本人と同定し、今回の照合率とメッセージダイジェストの組が過去の照合率とメッセージダイジェストの組と完全に一致した場合には本人と同定しないととも、過去の照合率とメッセージダイジェストの組と完全に一致する場合が、管理者の定める既定値以上に達した場合には、予め登録されている連絡先に通知するものである。

【0019】

【発明の実施の形態】以下図面を参照してこの発明の実施の形態を詳述する。

【0020】実施の形態1。図1にこの発明を適用したWebシステム1の構成を示す。ネットワーク2上に認証サーバ3、個人認証を必要とするアプリケーションサーバであるWebサーバ4、ユーザ端末5が接続され、ユーザ端末5にバイオメトリクス取得装置6が接続される。このWebシステム1において、ユーザがユーザ端末5を通じてWebサーバ4にアクセスした場合に、Webサーバ4はそのユーザの個人認証を認証サーバ3から受け、その結果によりユーザに対してアクセス制御を行う。

【0021】認証サーバ3は、認証制御部3A、暗号処理部3Cと、認証情報データベース3Bから構成されるパーソナルコンピュータやワークステーション等のコンピュータ装置（以下構成としてCPU、メモリ、ディスク、通信制御等を有するものを示す）であり、公開鍵方式の一方の鍵を公開鍵として公開し、もう一方を秘密鍵として秘匿している。

【0022】また、Webサーバ4は、Webサーバデータベース4A、暗号処理部4D、認証依頼部4Bと、

個人認証を必要とするアプリケーションであるWebサーバソフトウェア4C（以下ソフトウェアは、S/Wと記述する）のアプリケーションが動作するパーソナルコンピュータやワークステーション等のコンピュータ装置である。

【0023】また、ユーザ端末5は、Webサーバ端末4の情報を表示するブラウザ5Aと、認証情報取得S/W5Bが動作するパーソナルコンピュータやワークステーション等のコンピュータ装置である。またユーザ端末5には、バイオメトリクス取得装置6が接続されている。バイオメトリクス取得装置6は、画像処理等により人体の指紋や掌紋情報をバイオメトリクス情報として取得する、指紋取得装置7や、掌紋取得装置8、ユーザが描いた筆跡情報をバイオメトリクス情報として取得する文字認識タブレット9、眼底スキャンに等によって人体の網膜情報をバイオメトリクス情報として取得する網膜取得装置10等を示している。

【0024】ここでは、バイオメトリクス取得装置6に指紋取得装置7を使用する場合を例として説明する。また、指紋取得装置7などバイオメトリクス取得装置6の取得するバイオメトリクス情報は、画像データや、静電データなど加工されていないイメージデータであっても、イメージデータから特徴などを抽出した特徴点データであってもよい。指紋取得装置7は、画像処理等により、指紋情報を取得し、ユーザ端末に転送する指紋情報取得部7Aと、指紋情報を暗号化する暗号処理部7Bと、認証サーバ3の公開鍵を取得する公開鍵取得部7Cから構成される。

【0025】次に動作について説明する。このようなWebシステム1における認証処理の流れを図2に示す。まずユーザがユーザ端末5で動作しているアプリケーションであるブラウザ5Aにより、Webサーバ4の機密度の高いWebサーバデータベース4Aの情報にアクセスした場合（SP5）について説明する。前記機密度の高い情報のアクセス制御を行なっているアプリケーションであるWebサーバS/W4Cは、該ユーザがアクセス権限を有すか否かの判定するためにユーザ認証をする必要がある。

【0026】ユーザ端末5の認証情報取得S/W4Cは、認証のために必要なバイオメトリクス情報である指紋情報を、指紋取得装置7から取得する（SP6）。この時他のS/W（認証情報を取得するドライバなどのソフトウェア）と協調して動作する場合もある。

【0027】ユーザ端末5の認証情報取得S/W5Bから指紋情報の取得を指示された、指紋取得装置7の指紋情報取得部7Aは、ユーザから指紋情報を取得する（SP1）。この指紋情報は、ユーザ固有の個人的な情報であるため、暗号処理部7Bで暗号化を実施するが、まず暗号処理部7Bは、この指紋情報を暗号化するための共通鍵方式の共通鍵を生成し、この共通鍵により指紋情報

を暗号化する。同時に暗号処理部 7 B は、日時情報を取得し、日時情報と共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに共通鍵で暗号化する (S P 2)。指紋取得装置 7 の公開鍵取得部 7 C は、フロッピーディスクや、磁気カード、IC カード、またはキー入力などユーザからの指示により認証サーバの公開鍵を得る。または指紋取得装置 7 が適切に管理されている場合には、認証サーバ 3 の公開鍵が指紋取得装置 7 で固定的に公開鍵取得部 7 C に格納されており、ユーザが認知した上でその公開鍵を用いる場合もある。次に暗号処理部 7 B は前記共通鍵を認証サーバ 3 の公開鍵で暗号化する (S P 3)。そして、指紋取得部 7 A は、暗号化された指紋情報と、日時情報と、暗号化された日時情報と共通鍵を連結してメッセージダイジェストと、暗号化された共通鍵を認証情報としてユーザ端末 5 の認証情報取得 S/W 5 B に転送する (S P 4)。

【0028】ユーザ端末 5 の認証情報取得 S/W 5 B は、ブラウザ 5 A を介して Web サーバ 4 へ取得した認証情報を転送する。この時、ブラウザ 5 A は別途取得したユーザ名やメールアドレスなどのユーザ ID を認証情報に追加して転送する (S P 7)。

【0029】Web サーバ 4 の認証依頼部 4 B は、Web サーバ S/W 4 C を介して取得した認証情報を認証サーバ 3 の認証制御部 3 A へ転送する (S P 9)。

【0030】認証サーバ 3 の認証制御部 3 A は転送された認証情報を暗号処理部 3 C で復号させ、ユーザ認証を実施する。この時暗号処理部 3 C では、認証サーバ 3 で転送された日時情報と共通鍵からメッセージダイジェストを作成したものと、暗号化された日時情報と共通鍵を連結したメッセージダイジェストを復号したものを比較して、転送遅延を考慮した上で認証情報作成日時の正当性を確認する (S P 12)。認証制御部 3 A は転送された認証情報に含まれる指紋情報とユーザ ID と、認証サーバ 3 の認証情報データベース 3 B に元々蓄積されている個人情報から指紋照合を実施する。認証制御部 3 A は、照合した結果本人と同定した場合には、正規ユーザを示す認証結果を生成し、照合の結果本人と同定できなければ、本人ではないと判断し認証結果を生成する。この認証結果は、暗号処理部 3 C に引き渡され、暗号処理部 3 C では認証結果のメッセージダイジェストをとり、認証サーバ 3 の秘密鍵で暗号化、すなわちデジタル署名を行い、この暗号化されたメッセージダイジェストを認証制御部 3 A へ引き渡す。認証制御部 3 A は前記暗号化されたメッセージダイジェストを認証結果に含めて Web サーバ 4 の認証依頼部 4 B へ通知する (S P 13)。

【0031】認証結果を受けた Web サーバ 4 の認証依頼部 4 B は、暗号処理部 4 D に認証結果を通知する。暗号処理部 4 D は通知された暗号化されたメッセージダイジェストを認証サーバ 3 の公開鍵で復号し、通知された認証結果のメッセージダイジェストと比較することによ

り、確かに正当な認証サーバ 3 からの通知であることを確認する (S P 10)。認証依頼部 4 B は正当な認証サーバ 3 からの通知であることを確認したことを暗号処理部 4 D から知らされたならば認証結果を Web サーバ S/W 4 C に通知する。Web サーバ S/W 4 C は該認証結果により該ユーザに対して Web サーバデータベース 4 A の機密度の高い情報へのアクセス許可・不許可を判定する (S P 11)。たとえば、該機密情報の表示を行なうなど、ユーザアクセスに対する動作を行なう。

10 【0032】このように、ユーザの個人情報である指紋情報は生成した共通鍵で暗号化され、該共通鍵は、ユーザが設定した認証サーバ 3 の公開鍵により暗号化されることと、認証サーバ 3 の公開鍵は指紋取得装置 7 にユーザが直接設定するため、指紋情報はユーザの指定した認証サーバ 3 にのみ復号可能な状態でネットワーク上を転送されることになるので、バイオメトリクス情報である指紋情報というユーザ個人のプライバシーを、ユーザの意志を反映した形で確実に保護できるという効果がある。さらに、ユーザは認証サーバ 3 の公開鍵のみをフロッピーディスクや、磁気カード、IC カード、またはキー入力などで指紋取得装置 7 に指示できるようにすればよく、この公開鍵を格納しているフロッピーディスクや、磁気カード、IC カードなどが紛失や盗難にあってもセキュリティ上問題がなく、同じ公開鍵を格納した代替品や同一品により個人認証を受けることができる。この公開鍵を格納している代替品はユーザ毎に管理されているものではないため、紛失や盗難時に特別な届け出や再発行などの処理が不要であり、管理負荷が軽減できるとい

30 【0033】また、認証サーバ 3 で認証情報作成時の日時が確認するため、不正な認証情報の再使用が防止でき、認証情報認証サーバ 3 によって認証されたかが認証依頼側の Web サーバ 4 で確認できるためセキュリティを高く保つことが可能である。

【0034】本実施例では Web システム 1 に適用した例を示したが、Web サーバ S/W 4 C とブラウザ 5 A が、例えば経理情報管理サーバ S/W と経理情報管理クライアント S/W であったり、データベース検索サーバ S/W とデータベース検索クライアント S/W など他のシステムを構成するアプリケーションであっても同様な効果が得られる。

40 【0035】実施の形態 2. この実施の形態 2 においては実施の形態 1 を簡略したものであり、図 1 の Web サーバ 4 とユーザ端末 5 は図 3 のユーザ端末 5 の 1 つになる。図 1 との対応部分に同一符号を付けた図 3 では、個人認証を必要とするアプリケーションがユーザ端末 5 にのみ存在するため、図 1 の Web サーバ S/W 4 C とブラウザ 5 A のシステムを構成する 2 つのアプリケーションが 1 つのデータベース検索 S/W 5 E に置き換わり、Web サーバデータベース 4 A はローカルデータベース

5Cに置き換わる場合である。この場合図1のWebサーバ4を構成していた認証依頼部4Bと暗号処理部4Dは、図3のユーザ端末5の構成部位となる。

【0036】実施の形態2においては、ユーザ端末5は、ローカルデータベース5C、暗号処理部5F、認証依頼部5Dと、個人認証を必要とするアプリケーションであるデータベース検索S/W5E、認証情報取得S/W5Bが動作するパーソナルコンピュータやワークステーション等のコンピュータ装置である。またバイオメトリクス取得装置6はユーザ端末5に接続されており、上述した実施の形態1と全く同様の構成である。また認証サーバ3も、上述した実施の形態1と全く同様の構成である。

【0037】ここでは、バイオメトリクス取得装置6に指紋取得装置7を使用する場合を例として説明する。

【0038】次に動作について説明する。基本的には実施例1と同じであり、図2との対応部分に同一符号を付けた図4において、まずユーザがユーザ端末5で動作しているアプリケーションであるデータベース検索S/W5Eにより、機密度の高いローカルデータベース5Cの10 情報にアクセスした場合について説明する。前記機密度の高い情報のアクセス制御を行なっているアプリケーションであるデータベース検索S/W5Eは、該ユーザがアクセス権限を有するか否かの判定するためにユーザ認証をする必要がある(S/P5)。

【0039】ユーザ端末5の認証情報取得S/W5Bは、認証のために必要なバイオメトリクス情報である指紋情報を、指紋情報取得装置7から取得する(S/P6)。この時他のS/W(認証情報を取得するドライバなどのソフトウェア)と協調して動作する場合もある。20

【0040】ユーザ端末5の認証情報取得S/W5Bから指紋情報の取得を指示された、指紋取得装置の認証情報取得部7Aは、ユーザから指紋情報を取得する(S/P1)。この指紋情報は、ユーザ固有の個人的な情報であるため、暗号処理部7Bで暗号化を実施するが、まず暗号処理部7Bは、この指紋情報を暗号化するための共通鍵方式の共通鍵を生成し、この共通鍵により指紋情報を暗号化する。同時に暗号処理部7Bは、日時情報を取得し、日時情報と共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに共通鍵で暗号化する(S/P2)。指紋取得装置7の公開鍵取得部7Cは、フロッピーディスクや、磁気カード、ICカード、またはキー入力などユーザからの指示により認証サーバ3の公開鍵を得る。または指紋取得装置7が適切に管理されている場合には、認証サーバ3の公開鍵が指紋取得装置7で固定的に公開鍵取得部7Cに格納されており、ユーザが認知した上でその公開鍵を用いる場合もある。次に暗号処理部7Bは前記共通鍵を認証サーバ3の公開鍵で暗号化する(S/P3)。そして、指紋取得部7Aは、暗号化された指紋情報と、日時情報と、暗号化

された日時情報と共通鍵を連結してメッセージダイジェストと、暗号化された共通鍵を認証情報としてユーザ端末5の認証情報取得S/W5Bに転送する(S/P4)。

【0041】ユーザ端末5の認証情報取得S/W5Bは、ユーザ名やメールアドレスなどのユーザIDを取得して認証情報に追加する(S/P7)。

【0042】認証依頼部5Dはこの認証情報を認証サーバ3の認証制御部3Aへ転送する(S/P7)。

【0043】認証サーバ3の認証制御部3Aは転送された認証情報を暗号処理部3Cで復号させ、ユーザ認証を実施する。この時暗号処理部3Cでは、認証サーバ3で転送された日時情報と共通鍵からメッセージダイジェストを作成したものと、暗号化された日時情報と共通鍵を連結したメッセージダイジェストを復号したものを比較して、転送遅延を考慮した上で認証情報作成日時の正当性を確認する(S/P12)。認証制御部3Aは転送された認証情報に含まれる指紋情報とユーザIDと、認証サーバ3の認証情報データベース3Bに元々蓄積されている個人情報から指紋照合を実施する。認証制御部3Aは、照合した結果本人と同定した場合には、正規ユーザを示す認証結果を生成し、照合の結果本人と同定できなければ、本人ではないと判断し認証結果を生成する。この認証結果は、暗号処理部3Cに引き渡され、暗号処理部3Cでは認証結果のメッセージダイジェストをとり、認証サーバ3の秘密鍵で暗号化、すなわちデジタル署名を行い、この暗号化されたメッセージダイジェストを認証制御部3Aへ引き渡す。認証制御部3Aは前記暗号化されたメッセージダイジェストを認証結果に含めてユーザ端末5の認証依頼部5Dへ通知する(S/P13)。

【0044】認証結果を受けたユーザ端末5の認証依頼部5Dは、暗号処理部5Fに認証結果を通知する。暗号処理部5Fは通知された暗号化されたメッセージダイジェストを認証サーバ3の公開鍵で復号し、通知された認証結果のメッセージダイジェストと比較することにより、確かに正当な認証サーバ3からの通知であることを確認する(S/P10)。認証依頼部5Dは正当な認証サーバ3からの通知であることを確認結果を暗号処理部5Dから知らされたならば認証結果をデータベース検索S/W5Eに通知する。データベース検索S/W5Eは該20 認証結果により該ユーザに対してローカルデータベース5Cの機密度の高い情報へのアクセス許可・不許可を判定する。たとえば、該機密情報の表示を行なうなど、ユーザアクセスに対する動作を行なう(S/P11)。

【0045】このような構成によれば、ユーザ端末5が認証サーバ3へ個人認証を依頼する場合において、上述した実施例1と同一の効果を得ることができる。

【0046】本実施例ではデータベース検索システム1に適用した例を示したが、データベース検索S/Wが、例えば経理情報管理S/Wなどの他のシステムを構成するアプリケーションであっても同様な効果が得られる。50

【0047】実施の形態3. この実施の形態3においては実施の形態1におけるバイオメトリクス取得装置6である指紋取得装置7の暗号処理部7Bと公開鍵取得部7Cがユーザ端末5にある形態である。

【0048】図1との対応部分に同一符号を付けた図5では、ユーザ端末5は、Webサーバ端末4の情報を表示するブラウザ5Aと、指紋情報を暗号化する暗号処理部5Fと、認証サーバ3の公開鍵を取得する公開鍵取得部5G、認証情報取得S/W5Bが動作するパーソナルコンピュータやワークステーション等のコンピュータ装置である。またユーザ端末5には、バイオメトリクス取得装置6が接続されている。また認証サーバ3とWebサーバ4は、上述した実施の形態1と全く同様の構成である。

【0049】また、本実施の形態におけるバイオメトリクス取得装置6の取得するバイオメトリクス情報は、画像データや、静電データなど加工されていないイメージデータであっても、イメージデータから特徴などを抽出した特徴点データであってもよく、バイオメトリクス取得装置6はイメージデータを取得するだけのCPUが実装されない簡易な機器であってもよい。ここでは、バイオメトリクス取得装置6に指紋取得装置7を使用する場合を例として説明する。指紋取得装置7は、画像処理等により、指紋情報を取得し、ユーザ端末に転送する指紋情報取得部7Aで構成される。

【0050】次に動作について説明する。基本的には実施例1と同じであり、図2との対応部分に同一符号を付けた図6において、まずユーザがユーザ端末5で動作しているアプリケーションであるブラウザ5により、Webサーバ4の機密度の高いWebサーバデータベース4Aの情報にアクセスした場合について説明する(SP5)。前記機密度の高い情報のアクセス制御を行なっているアプリケーションであるWebサーバS/W4Cは、該ユーザがアクセス権限を有するか否かの判定するためにユーザ認証をする必要がある。

【0051】ユーザ端末5の認証情報取得S/W5Bは、認証のために必要なバイオメトリクス情報である指紋情報を、指紋取得装置7から取得する(SP6)。この時他のS/W(認証情報を取得するドライバなどのソフトウェア)と協調して動作する場合もある。

【0052】ユーザ端末5の認証情報取得S/W5Bから指紋情報の取得を指示された、指紋取得装置7の指紋情報取得部7Aは、ユーザから指紋情報を取得し(SP1)、ユーザ端末5の認証情報取得S/W5Bに転送する(SP4)。

【0053】ユーザ端末5の認証情報取得S/W5Bは、指紋情報は、ユーザ固有の個人的な情報であるため、暗号処理部5Fで暗号化を実施させる。まず暗号処理部5Fは、この指紋情報を暗号化するための共通鍵方式の共通鍵を生成し、この共通鍵により指紋情報を暗号

化する。同時に暗号処理部5Fは、日時情報を取得し、日時情報と共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに共通鍵で暗号化する。(SP2)。ユーザ端末5の公開鍵取得部5Gは、ハードディスクや、フロッピーディスク、磁気カード、ICカード、またはキー入力などユーザからの指示により認証サーバの公開鍵を得る。次に暗号処理部5Fは前記共通鍵を認証サーバ3の公開鍵で暗号化する(SP3)。そして、認証情報取得S/W5Bは、暗号化された指紋情報と、日時情報と、暗号化された日時情報と共通鍵を連結してメッセージダイジェストと、暗号化された共通鍵を認証情報として、ブラウザ5Aを介してWebサーバ4へ取得した認証情報を転送する。この時、ブラウザ5Aは別途取得したユーザ名やメールアドレスなどのユーザIDを認証情報に追加して転送する(SP7)。

【0054】Webサーバ4の認証依頼部4BはWebサーバS/W4Cを介して、取得した認証情報を認証サーバ3の認証制御部3Aへ転送する(SP9)。

【0055】認証サーバ3の認証制御部3Aは転送された認証情報を暗号処理部3Cで復号させ、ユーザ認証を実施する。この時暗号処理部3Cでは、認証サーバ3で転送された日時情報と共通鍵からメッセージダイジェストを作成したものと、暗号化された日時情報と共通鍵を連結したメッセージダイジェストを復号したものを比較して、転送遅延を考慮した上で認証情報作成日時の正当性を確認する(SP12)。認証制御部3Aは転送された認証情報に含まれる指紋情報とユーザIDと、認証サーバ3の認証情報データベース3Bに元々蓄積されている個人情報から指紋照合を実施する。認証制御部3Aは、照合した結果本人と同定した場合には、正規ユーザを示す認証結果を生成し、照合の結果本人と同定できなければ、本人ではないと判断し認証結果を生成する。この認証結果は、暗号処理部3Cに引き渡され、暗号処理部3Cでは認証結果のメッセージダイジェストをとり、認証サーバ3の秘密鍵で暗号化、すなわちデジタル署名を行い、この暗号化されたメッセージダイジェストを認証制御部3Aへ引き渡す。認証制御部3Aは前記暗号化されたメッセージダイジェストを認証結果に含めてWebサーバ4の認証依頼部4Bへ通知する(SP13)。

【0056】認証結果を受けたWebサーバ4の認証依頼部4Bは、暗号処理部4Dに認証結果を通知する。暗号処理部4Dは通知された暗号化されたメッセージダイジェストを認証サーバ3の公開鍵で復号し、通知された認証結果のメッセージダイジェストと比較することにより、確かに正当な認証サーバ3からの通知であることを確認する(SP10)。認証依頼部4Bは正当な認証サーバ3からの通知であることを確認したことを暗号処理部4Dから知らされたならば認証結果をWebサーバS/W4Cに通知する。WebサーバS/W4Cは該認証

結果により該ユーザに対してWebサーバデータベース4Aの機密度の高い情報へのアクセス許可・不許可を判定する。たとえば、該機密情報の表示を行なうなど、ユーザアクセスに対する動作を行なう(S P 11)。

【0057】このように、ユーザの個人情報である指紋情報は生成した共通鍵で暗号化され、該共通鍵は、ユーザが設定した認証サーバ3の公開鍵により暗号化されることと、認証サーバ3の公開鍵はユーザ端末5にユーザが直接設定するため、指紋情報はユーザの指定した認証サーバ3にのみ復号可能な状態でネットワーク上を転送されることになるので、バイオメトリクス情報である指紋情報というユーザ個人のプライバシーを、ユーザの意志を反映した形で確実に保護できるという効果がある。ただし、指紋情報がユーザ端末5では暗号化されずに存在する期間が生じるため、指紋取得装置7から暗号化される場合に比べてはセキュリティが低くなるが、ユーザ端末5自身が適切に管理されている場合には問題なく、指紋取得装置7に暗号処理部と公開鍵取得部が不要なため指紋取得装置7の構成が簡単になるという効果がある。前記した効果以外は、上述した実施例1と同様の効果を得ることができる。また、実施の形態2で示した、データベース検索S/W5Eなどのアプリケーションへも同様に適用でき、上述した同様の効果を得ることができる。

【0058】また、実施の形態1や、実施の形態2、実施の形態3の全ての場合において、取得したユーザのバイオメトリクス情報を暗号化するための共通鍵を生成を行うが、この共通鍵の解読を困難にするためには、共通鍵を生成するための乱数に傾向なくす必要がある。バイオメトリクス情報は一般に取得毎に異なった値をもつことから、取得したバイオメトリクス情報のメッセージダイジェストを乱数の一部または全部として利用する。

【0059】以上のように、取得したバイオメトリクス情報のメッセージダイジェストから生成する乱数を生成するので、生成した乱数の傾向をなくすことが簡単にできる。そして、この乱数の一部または全部を共通鍵の生成するための乱数として使用するので、認証回数や時刻などには全く関連ない乱数を発生させることができ、共通鍵の解読に対してセキュリティ上強固なシステムを構築することが可能である。

【0060】実施の形態4. 前記してきた、バイオメトリクス情報取得装置の管理は正当な管理者のみが実施できるが、正当な管理者を誰も認証できない状態に陥った場合には、前記認証されない管理者または管理を代行する他の者がバイオメトリクス取得装置の初期化を実行できる必要がある。この場合を実施の形態1と実施の形態2の指紋取得装置で、指紋取得装置が適切に管理されており、認証サーバの公開鍵が指紋取得装置で固定的に決まっている場合を例にして説明する。

【0061】図7は、指紋取得装置12の公開鍵取得部

12Cに固定的に格納される公開鍵を設定および変更など管理時の構成である。管理端末11は管理S/W11Aが動作するパーソナルコンピュータやワークステーション等のコンピュータ装置である。指紋取得装置12は指紋情報取得部12Aと暗号処理部12B、公開鍵取得部12Cと、管理部12Dで構成される。

【0062】管理端末11の管理S/W11Aは公開鍵設定を実行するため、指紋取得装置12に管理者の認証要求を発行する。指紋取得装置12の管理部12Dの管理者認証部12D1では、指紋情報取得部7Aから管理者の指紋を取得し管理者の指紋照合を行うが管理者と同一でない事態が発生したような状態に陥ることがありえる。これは管理者の怪我により、指紋自体がなくなってしまった場合などが相当する。この場合、管理S/W11Aは指紋取得装置12の管理部12Dの初期化者認証部12D2に対して初期化を命じるが、この時初期化用のパスワードなど事前に設定された手段により初期化者の認証を行う。初期化者認証部12D2は初期化者のみの認証しかせず、初期化者認証部12D2で認証時は指紋取得装置の初期化のみが実行できる。このように初期化者のための認証手段を通常の管理者と別に備えることにより、管理者が認証できなくなった場合や、管理者が突然いなくなったなどの場合においても初期化だけは実行できるとともに、初期化権限を保持していない者に不正に初期化されてしまうことを防げるという効果がある。

【0063】実施の形態5. 図8は、前述した認証サーバに、信頼性を向上するために不正認証を発見する手段を適用したものである。認証サーバ13は、履歴部13Dと、認証制御部13A、暗号処理部13Cと、認証情報データベース13Bから構成されるパーソナルコンピュータやワークステーション等のコンピュータ装置である。

【0064】認証サーバ13の履歴部13Dはユーザ認証時に、バイオメトリクスを照合した結果の照合率の履歴をとる。また、履歴部13Dは、同一ユーザ認証時で認証制御部13Aが本人と同一でない場合には、前回までのユーザを本人と同一とした時の平均照合率と比較し、今回の照合率が管理者の定める規定値以上に大きく変動しないことを確認する。履歴部13Dは、既定値以上に変動している場合には失敗回数を増加させる。そして失敗回数が管理者の定める既定値以上に達した場合には、予め登録されている管理者やユーザ自身に通知する。

【0065】この機構によれば、管理者に対してや、成り済まされようとしているユーザに対して、バイオメトリクス認証特有の異常な照合結果を通知するので、不正な認証の早期発見を可能にし、システムのセキュリティを高く保持することができる。

【0066】また、バイオメトリクスによる認証では、照合率が同一であってもバイオメトリクス情報は取得の

たびに異なった情報になるため、過去に取得したバイオメトリクス情報が一致することは確率的に非常に小さい。このバイオメトリクス認証の特徴を利用した不正発見の機構を説明する。図 8 の認証サーバ 13 の履歴部 13D はユーザ認証時、認証制御部 13A が本人と同定した場合には、前回までのユーザを本人と同定した時の照合率と比較し、同一の照合率であるかを確認する。同一であり、バイオメトリクス情報のメッセージダイジェストが格納されていない場合にはユーザ認証を失敗とすることを認証制御部 13A に通知し、認証制御部 13A は認証結果を失敗とする。同時に履歴部 13D はバイオメトリクス情報のメッセージダイジェストを照合率とともに格納する。同一の照合率で、メッセージダイジェストが格納されている場合には、今回のバイオメトリクス情報のメッセージダイジェストを算出し、過去の同一の照合率におけるバイオメトリクス情報のメッセージダイジェストと比較し、異なれば本人と同定するが、一致していれば成り済まされている可能性があるためユーザ認証を失敗とすることを認証制御部 13A に通知する。認証制御部 13A は認証失敗の認証結果を失敗とする。履歴部 13D は、照合率とメッセージダイジェストが一致して認証が失敗させた場合には照合率同一での失敗回数を増加させ、この失敗回数が管理者の定める既定値以上に達した場合には、予め登録されている管理者やユーザ自身に通知する。

【0067】この機構によれば、管理者に対してや、成り済まされようとしているユーザに対して、バイオメトリクス情報の漏洩による成り済ましと考えられる異常事態を通知するので、不正な認証の早期発見を可能にし、システムのセキュリティを高く保持することができる。また、履歴部 13D が記憶するのは 2 回目以降の同率照合率時のバイオメトリクス情報のメッセージダイジェストであるため、格納のための領域を削減できるという効果と、メッセージダイジェストによる比較のため、バイオメトリクス情報そのものを比較する場合にくらべて、比較に費やす時間を短くできるという効果がある。

【0068】

【発明の効果】以上のように、この発明によれば、ユーザの個人情報であるバイオメトリクス情報は暗号化され、バイオメトリクス情報はユーザの指定した認証サーバにのみ復号可能な状態でネットワーク上を転送されることになるので、バイオメトリクス情報というユーザ個人のプライバシーを、ユーザの意志を反映した形で確実に保護できるという効果があるとともに、認証サーバ 3 で認証情報作成時の日時が確認できるため、不正な認証情報の再使用が防止でき、さらに認証サーバによって認証されたかが認証依頼側で確認できるためシステムのセキュリティを高く保つことが可能である。

【0069】さらに、ユーザは認証サーバの公開鍵を指示するが、仮にこの公開鍵を格納しているフロッピーデ

ィスクや、磁気カード、ICカードなどが紛失や盗難にあってもセキュリティ上問題がなく、同じ公開鍵を格納した代替品や同一品により個人認証を受けることができるとともに、公開鍵を格納している代替品はユーザ毎に管理されているものではないため、紛失や盗難時に特別な届け出や再発行などの処理が不要であり、管理負荷が軽減できるという効果もある。

【0070】また、取得したバイオメトリクス情報から共通鍵の生成するための乱数を生成するので、認証回数や時刻などには全く関連ない乱数を発生させることができ、共通鍵の解読に対してセキュリティ上強固なシステムを構築することが可能である。また、初期化者のための認証手段を通常の管理者と別に備えることにより、管理者が突然いなくなった場合などの場合においても初期化ができるとともに、初期化権限を保持していない者に不正に初期化されてしまうことを防げるという効果がある。

【0071】また、認証サーバはユーザ認証時の履歴をとり、予め指定された者に対して、バイオメトリクス認証特有の異常な照合結果を通知するので、不正な認証の早期発見を可能にし、システムのセキュリティを高く保持することができる。

【図面の簡単な説明】

【図 1】 この発明による遠隔認証システムを適用した Web システムの実施の形態 1 の構成を示すブロック図である。

【図 2】 図 1 の Web システムにおける認証の処理の説明に供するタイミングチャートである。

【図 3】 この発明による遠隔認証システムを適用したデータベース検索システムの実施の形態 2 の構成を示すブロック図である。

【図 4】 図 3 のデータベース検索システムにおける認証の処理の説明に供するタイミングチャートである。

【図 5】 この発明による遠隔認証システムを適用した Web システムの実施の形態 3 の構成を示すブロック図である。

【図 6】 図 5 の Web システムにおける認証の処理の説明に供するタイミングチャートである。

【図 7】 この発明による遠隔認証システムを適用した指紋取得装置の管理時の実施の形態 4 の構成を示すブロック図である。

【図 8】 この発明による遠隔認証システムを適用した認証サーバの実施の形態 5 の構成を示すブロック図である。

【符号の説明】

1 Web システム

2 ネットワーク

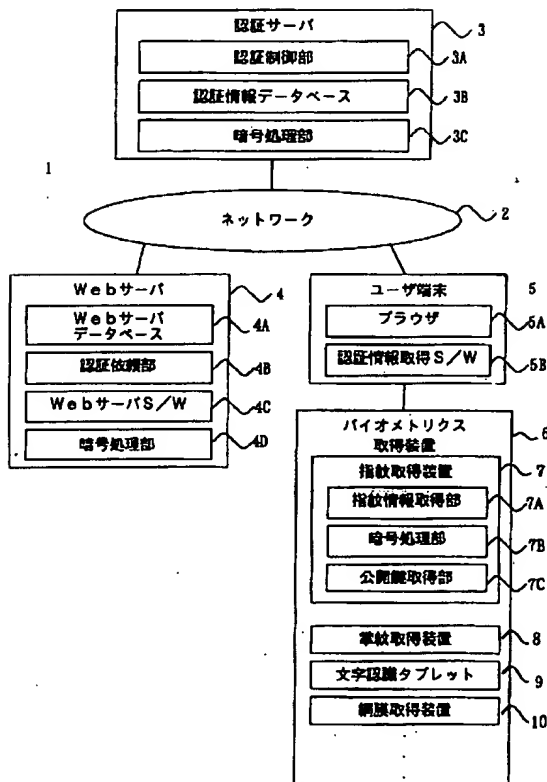
3 認証サーバ

3A 認証制御部

3B 認証情報データベース

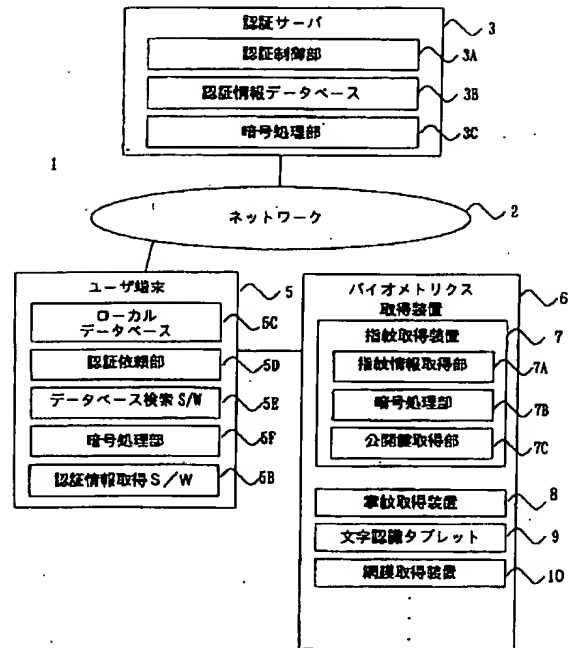
3C 暗号処理部
 4 Webサーバ
 4A Webサーバデータベース
 4B 認証依頼部
 4C Webサーバソフトウェア
 4D 暗号処理部
 5 ユーザ端末
 5A ブラウザ
 5B 認証情報取得ソフトウェア
 5C ローカルデータベース
 5D 認証依頼部
 5E データベース検索ソフトウェア
 5F 暗号処理部
 5G 公開鍵取得部
 6 バイオメトリクス取得装置
 7 指紋取得装置
 7A 指紋情報取得部
 7B 暗号処理部

【図1】

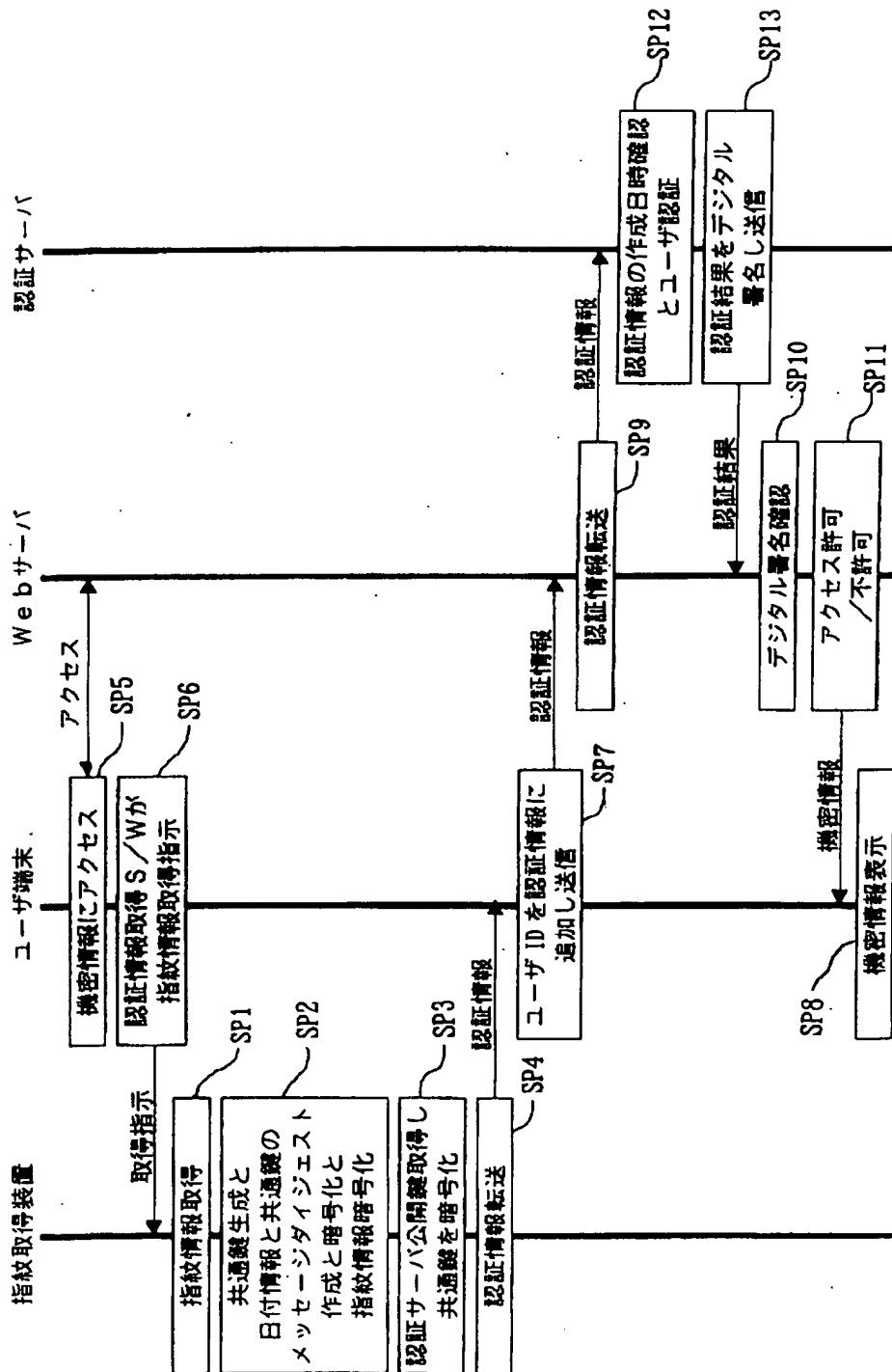


7C 公開鍵取得部
 8 掌紋取得装置
 9 文字認識タブレット
 10 網膜取得装置
 11 ユーザ端末
 11A 管理ソフトウェア
 12 指紋取得装置
 12A 指紋情報取得部
 12B 暗号処理部
 12C 公開鍵取得部
 12D 管理部
 12D1 管理者認証部
 12D2 初期化者認証部
 13 認証サーバ
 13A 認証制御部
 13B 認証情報データベース
 13C 暗号処理部
 13D 履歴部

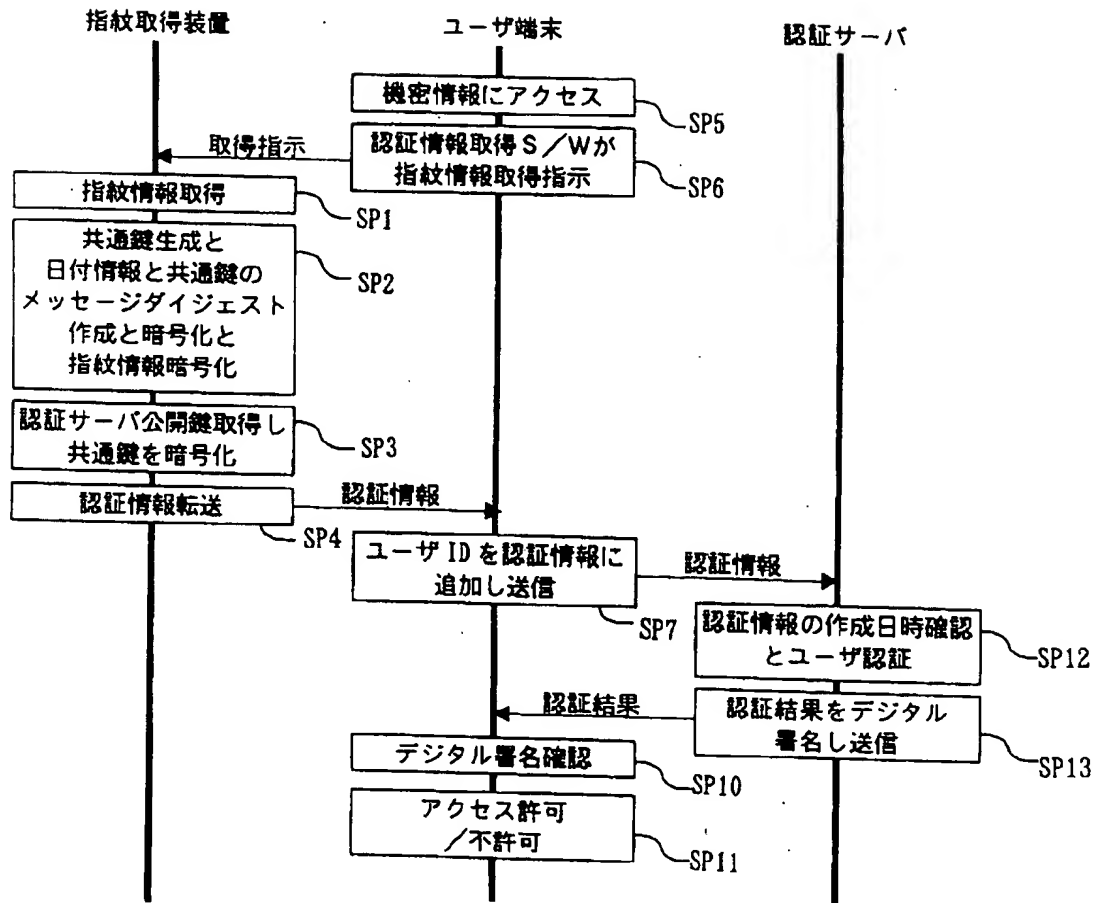
【図3】



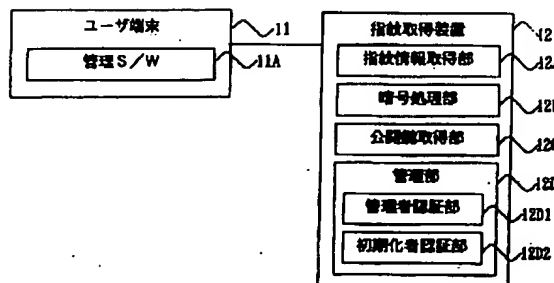
【図 2】



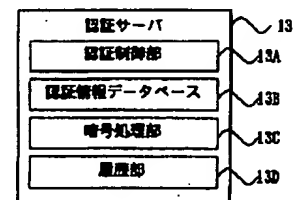
【図 4】



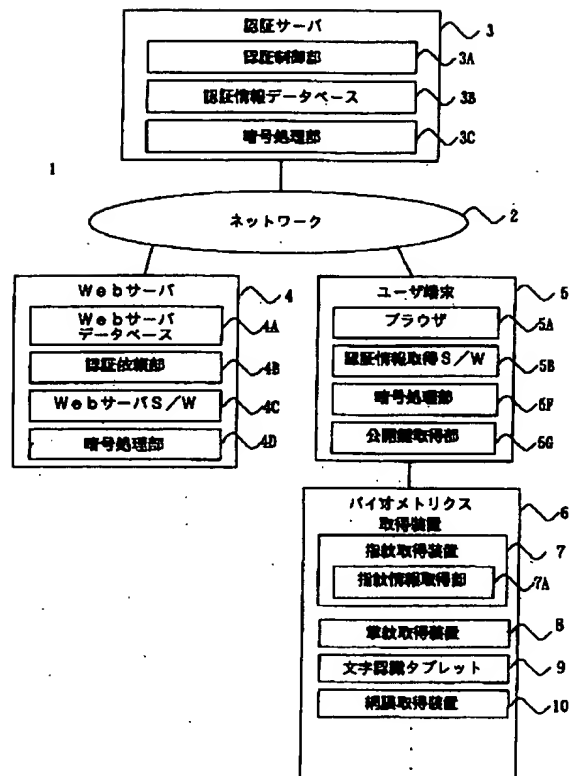
【図 7】



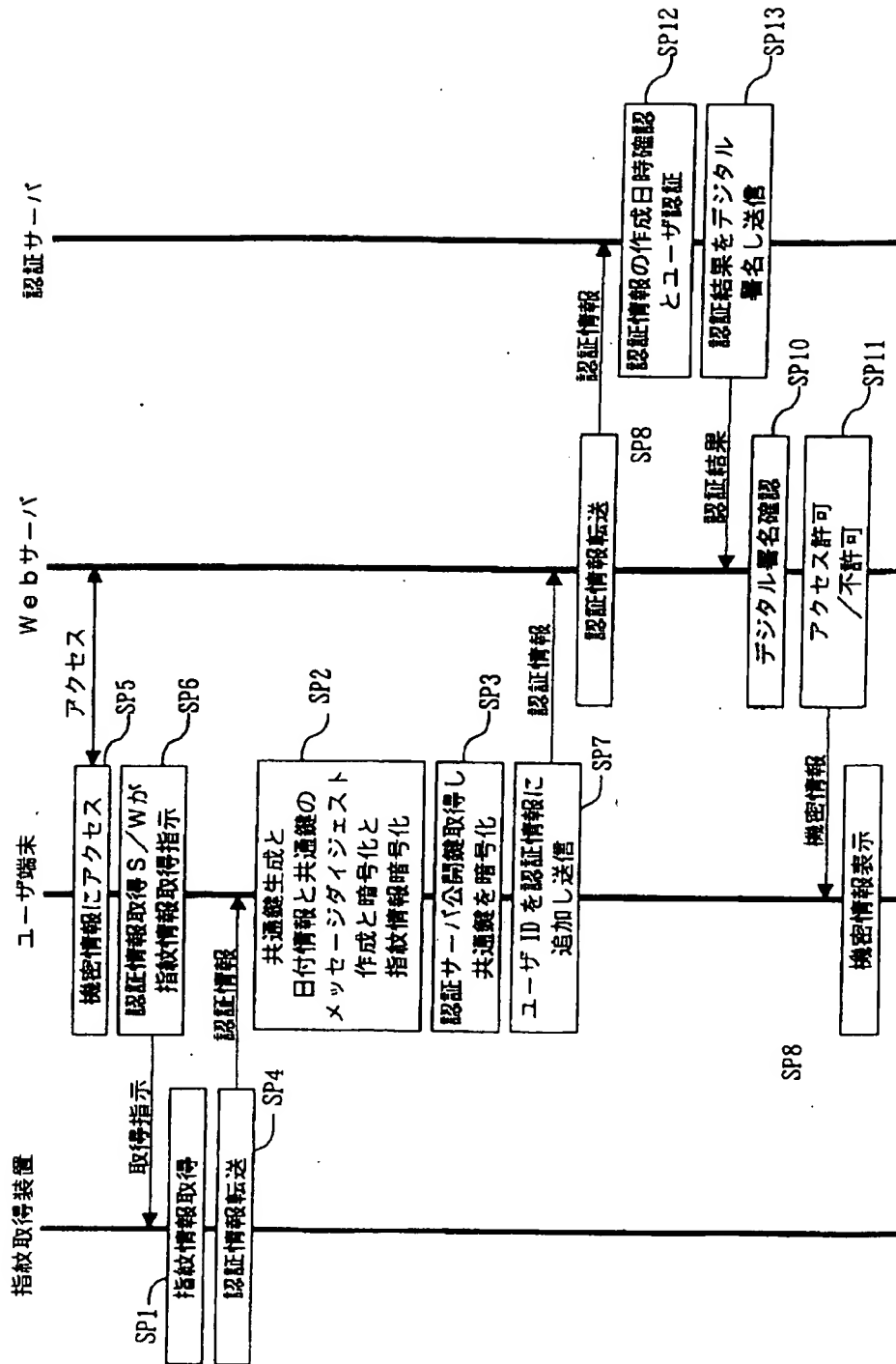
【図 8】



【図5】



【図 6】



フロントページの続き

(51) Int. Cl. ⁷

識別記号

F I

テーマコード* (参考)

H 0 4 L 9/00

6 7 5 D

(72) 発明者 貞包 哲男

東京都千代田区丸の内二丁目 2 番 3 号 三

菱電機株式会社内

F ターム (参考) 5B043 AA09 BA02 BA03 BA04 BA06

CA09 FA02 HA20

5B085 AC03 AE06 AE13 AE23 AE25

(72) 発明者 藤井 照子

東京都千代田区丸の内二丁目 2 番 3 号 三

菱電機株式会社内

AE29 BG07

5J104 AA07 EA01 EA19 KA01 KA16

MA02 NA02 PA07